UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,812	11/29/2005	Christophe Justin Evrard	550-619	4576

23117 7590 05/14/2007
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
VICARY, KEITH E	

ART UNIT	PAPER NUMBER
2183	

MAIL DATE	DELIVERY MODE
05/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,812	EVRARD ET AL.	
	Examiner	Art Unit	
	Keith Vicary	2183	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 April 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 April 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 are pending in this office action and presented for examination. Claims 1-3, 5-8, and 10 are newly amended by amendment filed 4/17/2007.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-2, 5-7, and 10 are rejected under 35 U.S.C. 102(e) as being anticipated by Qiu et al. (Qiu) (US 6804782 B1).

4. **Consider claim 1**, Qiu discloses an apparatus for processing data, comprising a process core (col. 4, lines 54-55, processor) operable to execute data processing instructions to generate result data values (col. 3, lines 24-28; mathematical operations); and

data processing registers holding data values defining state of said processor core to which said result data values are written (col. 7, lines 19-21, registers, line 37, temporary registers, lines 40-48, registers holding data values); wherein

at least one data processing instruction executed by said processor core is a conditional write data processing instruction (col. 3, lines 50-56 and col. 4, lines 1-5; the

multiplication operations; the storing of the result is conditional based on the private key) encoding condition codes specifying conditions under which said conditional write data processing instruction will or will not be permitted to write data to effect a change in state of said processor core (col. 4, lines 23-32 and 61-63, col. 5, lines 22-32; the cryptographic key determines the conditions under which the multiplication operation is emulated or not; note that the arguments section below explains the instruction encoding condition codes): and further comprising

a trash register to which a result data value may be written instead of a data processing register upon execution of said conditional write data processing instruction when said condition codes within said conditional write data processing instruction do not permit a write to effect a change in state of said processor core (col. 3, lines 28-31, store to memory that is unnecessary and lines 61-65, always performed the multiplication regardless of the value of the bit, col. 4, lines 1-11, 23-35 and col. 5, lines 37-47; the second memory correlates to the trash register).

5. **Consider claim 6**, Qiu discloses a method of processing data, comprising generating result data values upon execution by a processor core of data processing instructions (col. 4, lines 54-55, processor, and col. 3, lines 24-28; mathematical operations), at least one data processing instruction executed being a conditional write data processing instruction (col. 3, lines 50-56 and col. 4, lines 1-5; the multiplication operations; the storing of the result is conditional based on the private key) encoding condition codes specifying conditions under which said conditional write data

processing instruction will or will not be permitted to write data to effect a change in state of said processor core (col. 4, lines 23-32 and 61-63, col. 5, lines 22-32; the cryptographic key determines the conditions under which the multiplication operation is emulated or not; note that the arguments section below explains the instruction encoding condition codes) and wherein

a result data value is not written to a data processing register holding a data value defining state of said processor core (col. 7, lines 19-21, 37, 40-48, registers storing variables used by the algorithm, temporary register); when condition codes within said condition write data processing instruction do not permit a write to effect a change in state of said processor core but is instead written to a trash register (col. 3, lines 28-31, store to memory that is unnecessary and lines 61-65, always performed the multiplication regardless of the value of the bit, col. 4, lines 1-11, 23-35 and col. 5, lines 37-47; the second memory correlates to the trash register).

6. **Consider claims 2 and 7**, Qiu discloses said data processing register is part of a register bank having a plurality of data registers to which result data values are written (col. 5, lines 37-47; together the first memory and the second memory make up one bank in the same overall location as in Figure 4; also note that as in claims 1 and 6 above, the later mentioned registers are one embodiment of these memories).

7. **Consider claims 5 and 10**, Qiu discloses said trash register is part of said register bank (col. 5, lines 37-47; together the first memory and the second memory

make up one bank in the same overall location as in Figure 4), said trash register being unmapped to a register number such that said trash register may not be specified by a register specifying operand value (col. 5, lines 37-47; given that the second memory is used exclusively for when unnecessary stores to memory are required, and an unnecessary store is only deemed unnecessary based on the cryptographic key, and not based on any arguments/parameters in the instruction, it is inherent that the second memory cannot be specifically specified as an operand. Furthermore, in col. 7, lines 21-23 and 43-45, the unnecessary store is stored in a temporary register, which is well-known in the art to mean a register which is not user-addressable but is instead used for intermediate calculations).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 3-4 and 8-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Qiu as applied to claims 1-6 above, and further in view of Kissell (US 6625737 B1).

10. **Consider claims 3 and 8**, Qiu does not explicitly disclose that writing to said trash register is programmably disabled by a trash register control signal, although he does state that the total number of emulated operations, and thus the number of write

operations to the second memory, can be controlled (col. 1, lines 52-54, col. 6, lines 64-67 and col. 7, lines 1-8).

Although it would have been obvious to disable unnecessary storing by using a simple control signal, Kissell nevertheless discloses that writing to said trash register is programmably disabled by a trash register control signal (col. 8, lines 10-23, 41-46; the inhibit/burn signal line controls the power consumption of the processor by turning on/off subsystems, analogous to how the trash register control signal would turn on/off the multiplication/storing subsystem).

Kissel's selective disabling of subsystems reduces the power consumption of the processor (Kissel, col. 8, lines 44-46).

It would have been obvious to one of ordinary skill in the art at the time of the invention to use Kissel's teaching to save power. It would have been readily recognized to one of ordinary skill in the art at the time of the invention that the teaching of Kissel fits into the environment of Qiu as both deal with consuming extra power to mask attempts of differential power analysis.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teaching of Kissel with the invention of Qiu in order to selectively control the operation of the invention in case it is not necessary in order to save power.

11. **Consider claims 4 and 9**, Qiu does not explicitly disclose that said trash register control signal is stored in a system configuration register.

Although it would have been obvious to one of ordinary skill in the art at the time of the invention to store a signal that affects the operation of a processor in a system configuration register (such as an interrupt enable flag in a program status word register), Kissel nevertheless discloses that said trash register control signal is stored in a system configuration register (col. 8, lines 10-23; the maximum power threshold register essentially determines the value of the inhibit/burn signal).

It would have been readily recognized to one of ordinary skill in the art at the time of the invention that storing an operational parameter in a register takes less time to retrieve than storing in a memory.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use Qiu's teaching in order to increase system performance, as registers are faster than memory. It would have been readily recognized to one of ordinary skill in the art at the time of the invention that the teaching of Kissel fits into the environment of Qiu as both deal with consuming extra power to mask attempts of differential power analysis.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teaching of Kissel with the invention of Qiu in order to selectively control the operation of the invention with good response time, as storing an operational parameter in a register takes less time to retrieve than storing in a memory, in addition to the motivation set forth in claims 3 and 8.

Response to Arguments

12. Applicant's arguments filed 4/17/2007 have been fully considered but they are not persuasive. Examiner respectfully traverses applicants' remarks.

13. Applicant argues that Qiu does not modify the behavior of the conditional-write program instructions so as to write to one of a data processing register desired or a trash register; however, Qiu does do this; see the above rejection and response to arguments below. Applicant argues that the Qiu reference does not specify the requirement of a "trash register" as well as the requirement that a result data value is written to the trash register instead of to a data processing register when the condition codes within a conditional write data processing instruction do not permit a write to effect a change in state of the processor core; however, Qiu does do this; see the above rejection and response to arguments below.

14. Applicant expands on this argument by arguing the following three points.

15. Applicant argues that the cryptographic private key in Qiu which determines the conditional execution of the multiplication operation does not encode condition codes, and therefore, Qiu cannot be said to disclose the claimed "a conditional-write data processing instruction encoding condition codes." However, it would have been readily recognized to one of ordinary skill in the art at the time of the invention that an instruction may inherently encode condition codes in its opcode. For example, a branch-if-zero or branch-if-carry-set instruction inherently encodes condition codes in

the opcode or supplementing the opcode, depending on the specific implementation, which determines upon which conditions the instruction will execute. Regardless of the type of implementation, the branch-if-zero or branch-if-carry-set instruction still conditionally executes based on this condition code. For example, a branch instruction which uses 4 bits as an "opcode" and a fifth bit to signify that the branch should only take place if the zero flag is enabled in essence correlates to a branch-if-zero instruction which uses the aforementioned 5 bits combined together, with the last bit enabled, to signify the "opcode" for the branch-if-zero instruction, and a regular branch instruction which uses the aforementioned 5 bits combined together, with the last bit disabled, to signify the "opcode" for the branch instruction. Similarly, the cryptographic instructions serve as a conditional-write data processing instruction encoding condition codes, as the cryptographic instructions as a whole serve as the condition code and entail referring to the private key to determine whether to write to a first memory or not, just as a typical branch-if-zero instruction entails referring to the program status register to determine whether to branch or not.

16. Applicant argues that Qiu merely discusses a cryptography private key determining whether or not a multiplication operation should be carried out, but does not disclose an instruction encoding condition codes which determine whether or not that instruction will or will not be permitted to write data to effect a change in the state of the processor core, when that instruction is executed. However, as explained above, the cryptographic instruction inherently encodes the condition codes, the presence of which

cause the private key to be accessed in order to determine whether or not the instruction will or will not be permitted to write data to effect a change in the state of the processor core, as disclosed above. In both cases, a determination to write data which affects a change in the state of said processor core is made in response to encountering the data processing instruction, and the result of the determination is dependent on whether a condition is true or false.

17. Applicant argues that Qiu's teaching that the decision is to carry out a mathematical operation or not is not the same thing as the claimed invention of deciding to send a result data value to one of a trash register or the data processing register. However, as disclosed above in the rejection, Qiu does carry out a mathematical operation and then decides where to send the result data. Applicant may be trying to argue that that applicant's invention first executes the instruction, and then dependent on the condition codes, either writes to a trash register or to a data processing register. However, it is first noted that the current claims do not explicitly state that sequence of events. Furthermore, it is noted that Qiu's invention, which evaluates the condition, executes the instruction, and writes the data dependent on the condition, corresponds to the applicant's invention which executes the instruction, evaluates the condition, and writes the data dependent on the condition; although the order of the first two steps change, the results are nevertheless the same, as the same instruction gets executed regardless of the condition, as shown in, for example, col. 3, line 64 of Qiu (**the** multiplication) or col. 6, lines 9-13 of Qiu (the normal multiplication is implemented).

Applicant cites col. 4, lines 28-35 of Qiu, but it is noted that the mathematical operation is always performed; whether the operation is *necessary* or not is what the private key determines in order to determine where to store the result of the operation.

18. Applicant argues that no motivation was provided for combining the Qiu and Kissell references. However, see the rejection above for the motivations as in the first office action.

19. Applicant argues that Qiu's teaching of performing the mathematical operation or not performing it teaches away from the claimed invention; however, as explained above, Qiu does teach always performing the mathematical operation.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Keith Vicary whose telephone number is (571) 270-1314. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Eddie Chan can be reached on 571-272-4162. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

kv

EDDIE CHAN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100